Afdeling: Bestuur en Dienstverlening
Behandelaar: Wolf, Indra van der
Telefoonnummer: **959**

Voorstelnr. <Neem dossiernr over uit Ibabs>
Barneveld,
Portefeuillehouder: A.H. van de Burgwal

☐ Ter kennisname naar de raad
Nummer beleidsproduct:

☐ Op overzicht Bestaand beleid (website)

Onderwerp: **voorstel betreffende het vaststellen van het geactualiseerde privacybeleid**

Gevraagde beslissing:
1. Het beleidsstuk "Privacybeleid gemeente Barneveld 2021" vast te stellen door de burgemeester en het college van burgemeester en wethouders, ieder voor zover het hun bevoegdheid betreft en op 1 juni 2021 inwerking laten treden.

1. Inleiding
Op 1 april 2018 is het huidige Privacybeleid gemeente Barneveld in werking getreden. Nu we drie jaar verder zijn behoefde dit beleid met name een tekstuele actualisatie en update. Er zijn geen beleidsmatige veranderingen doorgevoerd. De grootste wijziging die is doorgevoerd is paragraaf 5.6 over data en ethiek.

2. Beoogd effect
Meetbaar effect: De gemeente Barneveld heeft aantoonbaar beleid, waarin wordt beschreven hoe er wordt omgegaan met de persoonsgegevens van betrokkenen.

Maatschappelijk effect: De gemeente Barneveld is richting betrokkenen transparant over de manier waarop de gemeente omgaat met persoonsgegevens. Dit kan het vertrouwen van betrokkenen in de gemeente versterken.

3. Argumenten
1. De gemeente Barneveld hecht er veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. Binnen de gemeente is hiervoor veel aandacht. Om de positie van het privacyvraagstuk verder te versterken is privacybeleid wenselijk. Dit privacybeleid is praktisch ingestoken en vormt een aanvulling op de verplichtingen die voortvloeien uit de AVG.

2. Met het privacybeleid is de gemeente Barneveld transparant over hoe zij omgaat met persoonsgegevens en draagt zij zorg voor een eenduidige werkwijze binnen de gemeente Barneveld.

3. Het gebruik van data neemt een steeds grotere vlucht en is niet meer weg te denken uit de samenleving. Naast privacy, speelt ook ethiek een (grote) rol bij het gebruik van data en innovaties. Daarom is nu in het beleid opgenomen hoe wij omgaan met data en ethiek.

4. Kanttekeningen
N.v.t.

5. Financiën
N.v.t.

6. Uitvoering

Planning: Het beleid treedt in werking na vaststelling door het college.

Communicatie: Het beleid wordt intern op intranet onder de aandacht gebracht.

Evaluatie/controle: Elk jaar voeren de Functionaris Gegevensbescherming en de Privacy Officer een zelfevaluatie uit, waarbij ook het beleid wordt geëvalueerd.

7. Bijlagen
1. Privacybeleid gemeente Barneveld 2021
2. Overzicht van wijzigingen

Privacybeleid gemeente Barneveld 2021

Vastgesteld bij besluit van 11 mei 2021

Inhoud

1. Algemeen

1.1 Inleiding

In de maatschappij is privacy een onderwerp dat veel in de belangstelling staat. Daarnaast stellen nieuwe technologische ontwikkelingen, innovatieve voorzieningen en een steeds meer digitale werkomgeving andere eisen aan de bescherming van persoonsgegevens en privacy. Wij zijn ons hiervan bewust en zorgen ervoor dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het beschermen van gegevens en het verwerken van persoonsgegevens is een zeer relevant onderwerp voor de gemeente Barneveld. De gemeente verwerkt persoonsgegevens voor de dienstverlening aan inwoners en bedrijven, voor de uitvoering van haar taken en als werkgever voor haar medewerkers. Bij gegevensbescherming gaat het om het zorgvuldig, veilig en doelmatig verwerken van persoonsgegevens.

Persoonsgegevens zijn de gegevens over een geïdentificeerde persoon of gegevens waarmee een persoon geïdentificeerd kan worden. Hierbij kan gedacht worden aan een naam, adresgegevens, foto of e-mailadres. Maar ook indirecte gegevens kunnen persoonsgegevens zijn, zoals een kentekenplaat op een voertuig of een IP-adres. Gevoelige en bijzondere persoonsgegevens zijn persoonsgegevens zoals het BSN en informatie over iemands gezondheid of strafrechtelijke gegevens.

Privacy is samenvattend te omschrijven als respect voor de persoonlijke levenssfeer van een individu. Om te voorkomen dat een onnodige of te vergaande inbreuk wordt gemaakt op de persoonlijke levenssfeer, is onder meer bij wet voorzien in waarborgen.

Privacybeleid

De gemeente Barneveld hecht er veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. Binnen de gemeente is hiervoor veel aandacht. Om de positie van het privacyvraagstuk verder te versterken heeft het college van burgemeester en wethouders besloten dat privacybeleid wenselijk is. Dit privacybeleid is praktisch ingestoken en vormt een aanvulling op de verplichtingen die voortvloeien uit de Europese Algemene Verordening Gegevensbescherming (hierna: AVG). Het college van burgemeester en wethouders stelt dit beleid dan ook vast.

In dit beleid staan kaders beschreven voor het verwerken van persoonsgegevens, de bescherming van deze gegevens en de omgang met deze gegevens. De kaders gelden voor de gemeente, samenwerkingsverbanden die zijn of worden aangegaan en derden die zijn of worden ingeschakeld. Verder kan het beschermen van persoonsgegevens niet geborgd worden zonder adequate informatiebeveiliging. Het privacybeleid hangt daarom ook samen met het Informatiebeveiligingsbeleid. Dit privacy beleid treedt in werking op 1 juni 2021 en is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente Barneveld plaatsvinden.

Contact
Vragen met betrekking tot privacy, het privacybeleid of de overige wet- en regelgeving op het gebied van privacy kunnen gericht worden aan de Privacy Officer van de gemeente Barneveld: privacy@barneveld.nl.

1.2 Wetgeving
Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet voorkomen worden dat onnodige of te vergaande inbreuken op iemands persoonlijke levenssfeer worden gemaakt. De AVG en de Uitvoeringswet AVG bieden hiervoor het wettelijk kader.

De AVG zorgt onder andere voor versterking en uitbreiding van de privacyrechten van betrokkenen en meer verantwoordelijkheden voor de gemeente Barneveld. Met de naleving van het privacybeleid spant de gemeente Barneveld zich in om aan de AVG en de UAVG te voldoen. In dit privacybeleid zijn de in de AVG opgenomen definities integraal van toepassing.

2. Uitgangspunten
De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Alle communicatie over de verwerking van persoonsgegevens vindt duidelijk, begrijpelijk en in de Nederlandse taal plaats. Betrokkenen zijn er zelf verantwoordelijk voor om dit indien nodig te (laten) vertalen in een voor hen begrijpelijke taal.

Grondslag en verwerken
De gemeente zorgt ervoor dat
het verwerken van persoonsgegevens gebaseerd is op één van de grondslagen zoals benoemd in de AVG[1]. Met verwerken wordt onder meer het verzamelen, vastleggen, opslaan, opvragen, raadplegen of vernietigen van persoonsgegevens bedoeld[2].

Doelbinding
Voor de verwerking van persoonsgegevens plaatsvindt, wordt bepaald voor welk doel de persoonsgegevens worden verwerkt. Het doel moet duidelijk en zo specifiek mogelijk worden geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Verder mogen persoonsgegevens niet verwerkt worden voor een ander doel dan waarvoor zij zijn verkregen.

[1] Artikel 6 AVG
[2] Artikel 4 lid 2 AVG

Subsidiariteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

Dataminimalisatie
De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt of worden de gegevens geanonimiseerd of gepseudonimiseerd[3].

Bijzondere persoonsgegevens
Bijzondere persoonsgegevens mogen niet worden verwerkt, tenzij een wettelijke grondslag aanwezig is om op dit verbod een uitzondering te maken.

Integriteit, vertrouwelijkheid en informatiebeveiliging
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

3. Rollen en verantwoordelijkheden

3.1 College van burgemeester en wethouders

De verantwoordelijke voor de verwerking van persoonsgegevens is het college van burgemeester en wethouders (hierna: het college), de burgemeester, de ambtenaar van de burgerlijke stand, de Heffingsambtenaar of de Invorderingsambtenaar. Welk bestuursorgaan verantwoordelijk is, is afhankelijk van hetgeen waarop de verwerking van persoonsgegevens betrekking heeft.

Aan de burgemeester als bestuursorgaan is een aantal wettelijke taken toegekend. Wanneer in het kader van deze taken verwerking van persoonsgegevens plaatsvindt, valt dit onder zijn verantwoordelijkheid. Aan het college als bestuursorgaan is ook een aantal wettelijke taken toegekend. Wanneer in het kader van deze taken verwerking van persoonsgegevens plaatsvindt, valt dit onder de verantwoordelijkheid van het college. Namens het college is de portefeuillehouder met de portefeuille ‘Bedrijfsvoering’ het eerste aanspreekpunt.

[3] Geanonimiseerde gegevens zijn niet herleidbaar tot een persoon en gepseudonimiseerde gegevens zijn middels een koppeling te herleiden tot een persoon.

Verantwoording aan de gemeenteraad
Het college legt verantwoording af aan de gemeenteraad over de uitvoering en realisatie van beleid. Met ingang van 2018 neemt het college in de programmabegroting een passage op over de uitvoering en realisatie van het privacybeleid. Naast de jaarlijkse verantwoording in de programmabegroting heeft het college de algemene informatieplicht om de gemeenteraad te informeren over bijzonderheden.

3.2 Directie en afdelingshoofden

De eindverantwoordelijkheid voor de ambtelijke uitvoering van het privacybeleid ligt bij de directie van de gemeente. Tussen de directie, Functionaris Gegevensbescherming en de Chief Information Security Officer vindt elk kwartaal overleg plaats over privacy en informatiebeveiliging.

De directie rapporteert door middel van een periodieke kennisgeving aan de portefeuillehouder. Elk afdelingshoofd is binnen zijn afdeling verantwoordelijk voor de naleving van het privacybeleid en een zorgvuldige verwerking van persoonsgegevens.

Vastlegging privacybeleid
De burgemeester en het college van burgemeester en wethouders stellen het gemeentelijk privacybeleid vast, ieder voor zover het hun bevoegdheid betreft. Bij de vaststelling dan wel herziening van het privacybeleid zal de burgemeester of het college de adviezen van de Functionaris Gegevensbescherming in overweging nemen.

3.3 Functionaris voor de Gegevensbescherming

De functie van Functionaris Gegevensbescherming (hierna: FG) is wettelijk verplicht. De FG ziet toe op naleving van de privacywetgeving en het privacybeleid binnen de gemeente. Hiervoor is het noodzakelijk dat de FG zijn taken en plichten onafhankelijk vervult en geen instructies ontvangt met betrekking tot de uitoefening van zijn functie. De werkzaamheden die de FG uitvoert hebben een wettelijke grondslag in de AVG (artikel 39).

Taken FG:

- Informeren en adviseren van de organisatie en verwerkers over hun verplichtingen die zij hebben op grond van de AVG en overige regelgeving op het gebied van privacy en persoonsgegevens;
- Advisering van de burgemeester, het college en de directie;
- Toezien op naleving van AVG en overige regelgeving op het gebied van privacy en persoonsgegevens;
- Toezien op naleving van het privacybeleid;
- Rapporteren van bevindingen aan het college en directie;
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van medewerkers;
- Advisering met betrekking tot de gegevensbeschermingseffectbeoordeling, toezien op de uitvoering daarvan en adviseren over noodzakelijke vervolgacties;
- Bijhouden register verwerkingsactiviteiten;

- Advisering van de Privacy Officer (hierna: PO) en de Chief Information Security Officer (hierna: CISO);
- Advisering van de PO bij de afhandeling van ingewikkelde klachten;
- Samenwerken met de Autoriteit Persoonsgegevens (hierna: AP): contactpersoon en intermediair tussen het college en de AP zoals benoemd in de AVG;
- Ontwikkelen van professionele kwaliteit en deskundigheid.

De taken zoals hierboven uitgewerkt moeten bij de FG worden belegd. Een aantal taken kunnen echter ook in (nauwe) samenwerking met of door de PO en de CISO worden uitgevoerd. Hierover worden werkafspraken gemaakt. De FG blijft niettemin altijd eindverantwoordelijke.

Bevoegdheden FG
De FG heeft controlebevoegdheden tot zijn beschikking zoals beschreven in titel 5.2 van de Algemene wet bestuursrecht (hierna: Awb). Deze bevoegdheden zijn noodzakelijk voor de uitoefening van geloofwaardig en effectief toezicht. Tevens gelden ook de waarborgen en beperkingen zoals beschreven in titel 5.2 Awb. In de bijlage zijn de belangrijkste (wettelijke) bevoegdheden van de FG opgenomen.

De FG is te bereiken via fg@barneveld.nl.

3.4 Privacy Officer

De PO heeft een brede functie, waarbij de PO hoofdzakelijk dient als interne (juridische) ondersteuning van de gehele organisatie voor alle privacy gerelateerde vraagstukken en dilemma's.

Taken PO:
- Ondersteuning bieden aan de FG;
- Implementeren privacyregelgeving en privacybeleid in de organisatie;
- Zorgdragen voor kennisoverdracht en bewustwording in de gemeente;
- Advisering van de burgemeester, het college en de directie;
- Functioneren als (juridische) vraagbaak voor de organisatie;
- Advisering bij gegevensuitwisseling met derden;
- Uitvoeren van gegevensbeschermingseffectbeoordelingen;
- Feitelijke afhandeling van datalekken en het beheren van het register waarin datalekken worden geregistreerd:
    - Een datalek beoordelen op ernst en consequenties en vertrouwelijk behandelen.
    - Afhankelijk onder wiens verantwoordelijkheid het datalek valt de volgende personen informeren en adviseren over de afhandeling van het datalek:
        - De burgemeester;
        - De portefeuillehouder 'Bedrijfsvoering' die namens het college het eerste aanspreekpunt is;
        - De directie;
        - Het betrokken afdelingshoofd.

      Het gehele college van burgemeester en wethouders wordt geïnformeerd en geadviseerd als dat gelet op de aard en/ of ernst van een datalek noodzakelijk is.

- Afhankelijk van de aard en ernst van een datalek het verantwoordelijke bestuursorgaan, de burgemeester of het college in de persoon van de portefeuillehouder ‘Bedrijfsvoering’, informeren en adviseren over de registratie van een datalek en de melding hiervan bij de AP én met instemming van het verantwoordelijke bestuursorgaan het datalek registreren en melden bij de AP.
- Afhankelijk van de aard en ernst van een datalek de FG en CISO betrekken bij de afhandeling daarvan.

  De PO mag correctieve en/of preventieve maatregelen nemen nadat de PO het verantwoordelijke bestuursorgaan, de burgemeester of het college in de persoon van de portefeuillehouder ‘Bedrijfsvoering’, hierover heeft geïnformeerd en geadviseerd én instemming heeft van het verantwoordelijke bestuursorgaan om de correctieve en/of preventieve maatregelen te nemen. Indien een datalek vereist dat direct maatregelen worden getroffen, wordt de burgemeester en/ of de portefeuillehouder ‘Bedrijfsvoering’ over de genomen maatregelen zo spoedig mogelijk geïnformeerd. Het gehele college van burgemeester en wethouders wordt geïnformeerd en geadviseerd als dat gelet op de aard en/ of ernst van een datalek noodzakelijk is én geeft instemming aan de PO om de correctieve en/of preventieve maatregelen te nemen.

- In mandaat afhandelen van klachten met betrekking tot de verwerking van persoonsgegevens;
- In mandaat afhandelen van verzoeken van betrokkenen, zoals recht op informatie, rectificatie en recht van bezwaar;
- Het ontwikkelen van professionele kwaliteit en deskundigheid.

De PO is te bereiken via privacy@barneveld.nl.

3.5 Chief Information Security Officer

Persoonsgegevens kunnen niet geborgd worden zonder adequate informatiebeveiliging. De CISO draagt zorg voor de informatiebeveiliging. De werkzaamheden die de CISO uitvoert worden beschreven in het Informatiebeveiligingsbeleid. De CISO stuurt op en evalueert de naleving van het Informatiebeveiligingsplan. Concreet adviseert de CISO het management over informatiebeveiliging, mogelijke risico’s en de daarbij behorende mitigerende maatregelen. Dit zijn alle maatregelen die negatieve effecten van het besluit of handelen voorkomen of beperken.

Tevens is de CISO samen met de PO en indien nodig de FG, betrokken bij de afhandeling van een datalek. De CISO mag correctieve en/of preventieve maatregelen met betrekking tot informatiebeveiliging nemen en stemt dit af met de PO en indien nodig de FG. De maatregelen worden pas genomen nadat de CISO het verantwoordelijke bestuursorgaan, de burgemeester of het college in de persoon van de portefeuillehouder ‘Bedrijfsvoering’, hierover heeft geïnformeerd en geadviseerd én instemming heeft van het verantwoordelijke bestuursorgaan om de correctieve en/of preventieve maatregelen te nemen. Indien een datalek vereist dat direct maatregelen worden getroffen met betrekking tot informatiebeveiliging, wordt de burgemeester en/ of de portefeuillehouder ‘Bedrijfsvoering’ over de genomen maatregelen zo spoedig mogelijk geïnformeerd.

3.6 Medewerkers

Alle medewerkers hebben een eigen verantwoordelijkheid in het goed omgaan met persoonsgegevens en zijn verantwoordelijk om kennis te nemen van het privacybeleid, de maatregelen en procedures op het gebied van gegevensverwerking en dienen deze na te leven. Van iedereen binnen de gemeente Barneveld wordt verwacht dat zij zorgvuldig en integer omgaan met persoonsgegevens.

3.7 Ketenpartners en leveranciers

Ketenpartners

De (keten)partners waarmee wij samenwerken en tijdens het samenwerken persoonsgegevens worden gedeeld, zijn vaak zelf verantwoordelijk voor het voldoen aan alle geldende privacywetgeving. Het is aan de (keten)partner om te voldoen aan de AVG. Per samenwerking en proces wordt beoordeeld of er een overeenkomst moet worden afgesloten en zo ja, wat voor een overeenkomst. Dit kan een verwerkersovereenkomst, overeenkomst gegevensuitwisseling, een convenant of een andere vorm van een overeenkomst zijn. Wat in elk geval hierin terugkomt zijn afspraken over de eisen waar de gegevensuitwisseling en de beveiliging aan moeten voldoen.

Leveranciers

Wanneer wij als verwerkingsverantwoordelijke bij een externe partij een product of bepaalde diensten afnemen waarbij sprake is van het verwerken van persoonsgegevens , wordt een verwerkersovereenkomst afgesloten. Hierbij wordt de standaard verwerkersovereenkomst (van de IBD) gehanteerd die door de VNG is vastgesteld.

Het afdelingshoofd of de teamleider die een dergelijke uitbesteding, samenwerking of uitwisseling van persoonsgegevens aangaat, ziet toe op en is verantwoordelijk voor het afsluiten van een overeenkomst. Voor dit proces is een handleiding opgesteld welke beschikbaar is gesteld op intranet.

4. Borging en beheersing privacy

4.1 Controle en naleving

De FG stelt in samenwerking met de CISO een controleplan privacy en informatiebeveiliging op en voert op basis hiervan de controle uit op het rechtmatig en zorgvuldig verwerken van persoonsgegevens. De resultaten van deze controles worden gerapporteerd aan de gemeenteraad en directie. Indien de naleving van het beleid en/of de bescherming van data en privacy gegevens (ernstig) tekort schieten, bepaalt de directie of en welke sancties opgelegd moeten worden, binnen de kaders van de CAO en de wettelijke mogelijkheden. Tevens worden er naar aanleiding van incidenten / datalekken register audits uitgevoerd op bepaalde processen.

4.2 Privacy Impact Assessement/ Privacy by design/ Privacy by default

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens wordt een Privacy Impact Assessement (PIA) uitgevoerd voor verwerkingen die waarschijnlijk een verhoogd risico opleveren voor betrokkenen en/ of betreffen processen waarvan de AP heeft gesteld dat er verplicht een PIA

moet worden uitgevoerd. Deze beoordeling zorgt ervoor dat alle risico's van een verwerking (vroegtijdig) in kaart worden gebracht en maatregelen kunnen worden getroffen.

Privacy by design en default worden bij nieuwe processen en/ of applicaties als eis meegenomen. Dit wordt onder meer vormgegeven door deelname van de PO aan het Planatelier en het pro- actief handelen van collega's door de PO vroegtijdig te betrekken bij het ontwerpen en implementeren van nieuwe processen en/ of applicaties.

4.3 Bewustwording en ondersteuning

Het is belangrijk dat het college, leidinggevenden en medewerkers bewust met persoonsgegevens omgaan. Om bewustwording te realiseren is kennisoverdracht noodzakelijk. De FG, PO en CISO zorgen ervoor dat informatie over privacy en informatiebeveiliging blijvend onder de aandacht worden gebracht van de gehele organisatie. Dit vindt onder meer plaats door het geven van workshops, het aansluiten bij teamoverleggen, het plaatsen van berichten op intranet en het uitvoeren van ludieke acties

Om de medewerkers te instrueren in het omgaan met en verwerken van persoonsgegevens, zijn er procedures en werkinstructies beschikbaar voor medewerkers. Tevens wordt voorzien in adequate (juridische) ondersteuning van medewerkers door de PO.

4.4 Kwaliteitscyclus en evaluatie

VNG Realisatie heeft criteria ontwikkeld om de AVG te vertalen naar een kwaliteitscyclus voor privacy en informatiebeveiliging voor gemeentelijke processen in een borgingsproduct. De criteria zijn uitgewerkt in maatregelen die aangeven hoe aan een criterium kan worden voldaan. De criteria, en daarmee de maatregelen, zijn vervolgens ingedeeld in thema's om inzicht te krijgen waar de gemeente staat op het gebied van de AVG. Hiermee wordt inzicht verkregen in het beheer en de bescherming van persoonsgegevens en is overzichtelijk op welke punten eventueel nog niet (volledig) is voldaan aan de AVG. De 7 thema's die tezamen alle aspecten van gegevensbescherming afdekken zijn:

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

Het borgingsproduct wordt jaarlijks in Q3 door de FG en PO ingevuld. De uitkomsten hiervan zijn vervolgens input voor het jaarverslag van de FG, evaluatie van dit beleid en actiepunten voor het daarop volgende kalenderjaar.

5. Rechtmatige en zorgvuldige verwerking van persoonsgegevens

5.1 Grondslag, doelbinding en verwerking

Grondslag

De AVG zegt dat voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden op grond van één van de onderstaande grondslagen:

1. Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
2. Voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
3. Om een wettelijke verplichting na te komen;
4. Om de vitale belangen van de betrokkene te beschermen;
5. Voor de goede vervulling van een taak van algemeen belang of een aan de gemeente wettelijk opgedragen taak;
6. Wanneer de verwerking noodzakelijk is voor de behartiging van een gerechtvaardigd belang.

[4]

Doelbinding

Volgens de AVG mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. Veelal is het doel omschreven in de wet. Per verwerking moet worden afgewogen of de gegevens verwerkt mogen worden. Wanneer het gebruik van gegevens noodzakelijk is voor andere doelen dan waarvoor de gegevens zijn verzameld, dan mogen alleen met ondubbelzinnige toestemming van de betrokkene de gegevens worden verwerkt. Het kan voorkomen dat bij casussen binnen de domeinen van Openbare orde en Veiligheid en het Sociaal Domein, geen toestemming wordt verkregen voor het verwerken van gegevens. Daarom wordt in paragraaf 5.4 en 5.5 per domein aangegeven wanneer het mogelijk is om zonder toestemming van betrokkenen wel gegevens te verwerken, indien hiervoor een noodzaak is en wordt voldaan aan de vereisten van proportionaliteit en subsidiariteit.

[4] www.autoriteitpersoonsgegevens.nl

Verwerking
Op de verwerking van persoonsgegevens is de AVG van toepassing. De verwerking van persoonsgegevens is elke geheel of gedeeltelijke geautomatiseerde handeling met persoonsgegeven(s)[5]. In de AVG wordt verwerking wordt als volgt omschreven:

- Verzamelen, vastleggen en ordenen;
- Bewaren, bijwerken en wijzigen;
- Opvragen, raadplegen, gebruiken;
- Verstrekken door middel van doorzending;
- Verspreiding of enige andere vorm van ter beschikkingstellen;
- Samenbrengen, met elkaar in verband brengen;
- Afschermen, uitwissen of vernietigen van gegevens.

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

Wijze van verwerking
Bij de verwerking van persoonsgegevens gelden een aantal regels[6]:

- De verwerking moet in overeenstemming zijn met de wet;
- De verwerking moet zorgvuldig gebeuren;
- De persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf en waar mogelijk eenmalig uitgevraagd in het kader van deregulering en vermindering van de lastendruk bij de betrokkene;
- Persoonsgegevens worden alleen verzameld als het doel niet op een andere manier kan worden bereikt;
- Het verzamelen van persoonsgegevens staat in verhouding tot het doel. Er wordt dus niet meer gevraagd dan nodig;
- Persoonsgegevens worden alleen verwerkt door personen met een geheimhoudingsplicht;
- Op de verwerking van persoonsgegevens is tevens het Informatiebeveiligingsbeleid van toepassing.

5.2 Register van verwerkingen

Als organisatie, zowel als verwerkingsverantwoordelijk als verwerker, zijn wij verplicht voor het hebben van een register van verwerkingen[7]. In dit register moeten alle processen waarbij persoonsgegevens worden verwerkt zijn opgenomen. Het register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt en welke gegevens daarvoor worden gebruikt. Wat in het register van verwerkingen moet staan is opgenomen in artikel 30 van de AVG.

Het register van verwerkingen is een document dat altijd aan verandering onderhevig is. De meest recente versie wordt centraal en onder verantwoordelijkheid van de PO bijgehouden. Jaarlijks wordt het register van verwerkingen beoordeeld door de FG op volledigheid en juistheid. De afdelingshoofden zijn verantwoordelijk voor het doorgeven van tussentijdse wijzigingen in de verwerkingen en processen aan de beheerder van het register. Voor dit proces is een handleiding opgesteld welke beschikbaar is gesteld op intranet.

[5] Artikel 2 lid 1 AVG
[6] Artikel 5 AVG
[7] Artikel 30 AVG

5.3 Gegevensuitwisseling Openbare orde en Veiligheid

Binnen het domein van Openbare orde en Veiligheid zijn verschillende overheidsinstanties werkzaam zoals politie, Belastingdienst, het Parket en gemeenten. Elke instantie heeft zijn eigen bij wet vastgestelde taken en bevoegdheden.

Bij de bestrijding van ondermijnende criminaliteit kan sprake zijn van complexe problematiek, waarbij een integrale aanpak vanuit de verschillende overheidsinstanties noodzakelijk is. Overheidsinstanties moeten dan onderling informatie en expertise met elkaar kunnen uitwisselen. Hiertoe is een convenant[8] opgesteld door het LIEC[9], om het uitwisselen van informatie, expertise en krachten tussen overheidsinstanties mogelijk te maken. Het RIEC[10] vervult hierbij een verbindende rol tussen de verschillende overheidsinstanties.

5.4 Gegevensuitwisseling Sociaal Domein

Binnen het Sociaal Domein is per domein[11] strikt vastgelegd of gegevens uitgewisseld mogen worden met ander domeinen binnen het Sociale Domein. Daarnaast is in Barneveld een privacyreglement voor de Wmo en Jeugd opgesteld voor het uitwisselen van informatie[12].

Bij bepaalde casussen kan sprake zijn van complexe en domein overstijgende problematiek, waarbij het wenselijk kan zijn dat gegevens tussen de sectoren worden uitgewisseld in het belang van de cliënt of zijn omgeving. In dergelijke casussen kan aan de cliënt toestemming worden gevraagd of hun gegevens tussen de sectoren mogen worden uitgewisseld. Wanneer de cliënt hiervoor geen toestemming geeft én de betrokken gespreksvoerder maakt zich ernstige zorgen over de cliënt of zijn omgeving, dan kan de casus bij het casuïstiekoverleg worden ingebracht en/ of bij VeiligThuis worden gemeld. Indien de casus bij VeiligThuis wordt gemeld, dan gebeurt dit volgens de meldcode[13]. Binnen de gemeente Barneveld zijn hiervoor drie Meldcode – functionarissen aangesteld met wie de casus besproken kan worden. Op deze wijze is geborgd dat indien noodzakelijk en in het belang van de cliënt of zijn omgeving overleg kan plaatsvinden. Gesprekvoerders dienen zich wel altijd te houden aan de wetgeving die voor hun beroepsgroep toepasselijk is[14]. Wanneer bij een casus sprake is van zeer ernstige problematiek met politiek-bestuurlijke gevoeligheid en/ of een casus heeft gevolgen voor de openbare orde en veiligheid, dan worden de burgemeester en/ of de wethouder(s) over de casus geïnformeerd.

[8] Convenant ten behoeve van een Bestuurlijke en Geïntegreerde Aanpak van Georganiseerde Criminaliteit, Bestrijding van Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen
[9] Landelijk Informatie en Expertise Centrum
[10] Regionaal Informatie en Expertise Centrum
[11] Onder andere Wmo 2015, Jeugdwet, Participatiewet en de Leerplichtwet
[12] Privacyreglement Wmo 2015 en Jeugdhulp Gemeente Barneveld
[13] Meldcode Huiselijk geweld en kindermishandeling: https://www.rijksoverheid.nl/onderwerpen/huiselijk-geweld/meldcode
[14] Elke beroepsgroep heeft zijn eigen wetgeving waaraan zij zich dienen te houden. Wanneer dit niet gebeurt, dan kan dit consequenties hebben voor de uitvoering van hun beroep.

5.5 Bewaartermijnen

Op grond van de AVG gelden geen concrete bewaartermijnen. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerking, dan wel bewaard volgens de van toepassing zijnde wettelijke bewaartermijnen zoals de Archiefwet, van toepassing zijnde sectorspecifieke wetgeving of de selectielijst van de VNG[15]. Wanneer persoonsgegevens niet langer bewaard (mogen) worden, worden deze gegevens vernietigd of aangepast zodat personen daarmee niet langer geïdentificeerd kunnen worden.

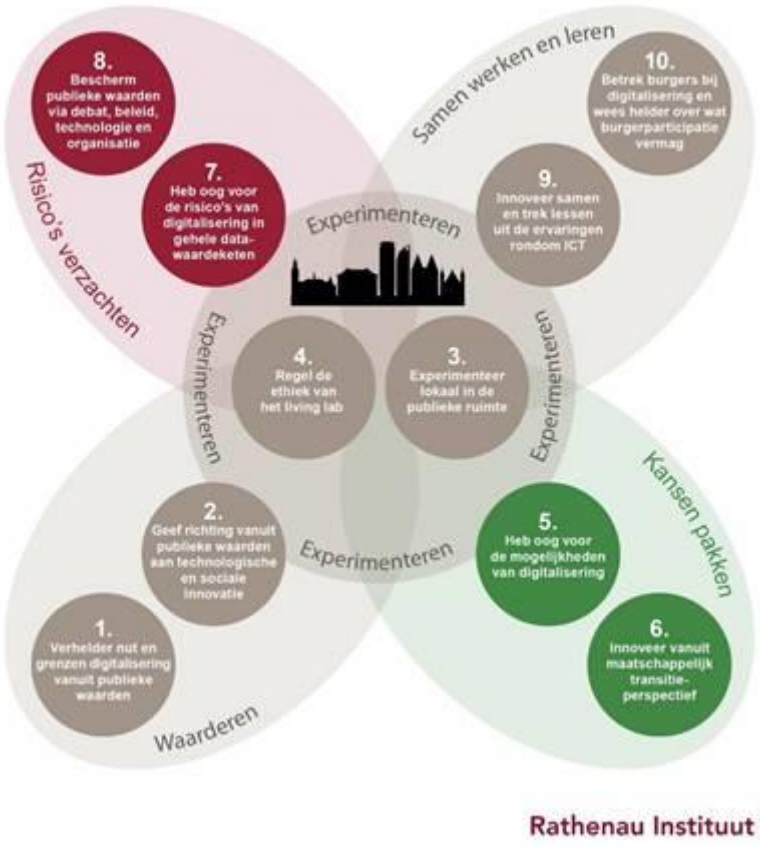
5.6 Data en ethiek

De wereld om ons heen verandert snel door alle technologische ontwikkelingen en innovaties. Datagedreven werken is voor veel organisaties niet langer slechts een 'nice to have' maar een 'must have'. De gemeente Barneveld wil naast innoveren, ook datagedreven werken. De eerste stappen hiertoe zijn inmiddels gezet met een Power BI dashboard voor Jeugd, het opstellen van profielen door AHTI[16] en het blockchainproject. Als gemeente beschikken we over een grote hoeveelheid data, naast de beschikbare (openbare) externe data. De stap van data naar inzicht is een hele grote. Laat staan van inzicht naar toepassing. Correlaties, koppeling en verbanden in gestructureerde en ongestructureerde data geven voorspellend vermogen en kunnen de kennis van de organisatie verstreken.

Maar het gebruik van data brengt ook ethische vraagstukken met zich mee: wat kunnen gevolgen en consequenties zijn van innovatie en datagedreven werken voor zowel medewerkers als inwoners? Om organisaties te helpen bij technologische innovatie en het gebruik van data heeft de universiteit Utrecht in samenwerking met data- analisten van de gemeente Utrecht een toolkit ontwikkeld, De Ethische Data Assistent (DEDA)[17]. Deze toolkit helpt bij het in kaart brengen van ethische kwesties bij het gebruik van data, het documenteren van het besluitvormingsproces en de bevordering van de verantwoording aan betrokken stakeholders zoals medewerkers en inwoners. Deze toolkit moeten wij als organisatie gebruiken om transparant te zijn bij innovaties en het gebruik van data en kennis op te doen over het gebruik van data.

Naast de toolkit heeft het Rathenau Instituut in opdracht van de VNG het rapport "Waardevol digitaliseren" uitgebracht[18]. Dit rapport legt een routekaart voor waaruit handelingsperspectieven volgen om digitalisering in de openbare ruimte vorm te geven. Zowel kansen als risico's van deze ontwikkelingen worden gaandeweg het proces ontdekt en in kaart gebracht. Deze routekaart hanteren wij naast de toolkit van DEDA. De stappen in deze routekaart zijn hieronder visueel gemaakt.

[15] https://vng.nl/artikelen/selectielijst
[16] Amsterdam health & technology institute
[17] https://dataschool.nl/deda/
[18] Waardevol digitaliseren | Rathenau Instituut



WAARDEREN

1. Verhelder nut en grenzen van digitalisering vanuit publieke waarden

Digitalisering kan ingezet worden voor verbetering van overheidsdiensten, versterking van burger-participatie en het stimuleren van economische innovatie en kennisopbouw. Tegelijkertijd kan het ook fundamentele publieke waarden onder druk zetten zoals privacy, autonomie en rechtvaardigheid. Bestuurders moeten vanuit dat perspectief duidelijk maken waarom of wanneer digitalisering gewenst is en waar er grenzen of randvoorwaarden aan gesteld moeten worden.

2. Geef richting vanuit publieke waarden aan technologische en sociale innovatie

Waar technologische kansen snel worden bejubeld, ontvangt men kritiek zelden met gejuich. Vernieuwen vraagt behalve om technologische ook om sociale innovatie. Bestuurders spelen hierbij een cruciale dubbelrol: stimuleren en richting geven vanuit publieke waarden.

EXPERIMENTEREN

3. Experimenteer lokaal in de publieke ruimte

Een experiment dat past bij innoveren vanuit een maatschappelijke uitdaging is het living lab. Een levensechte experimenteer omgeving waar onderzoekers, ondernemers, professionals, gebruikers, beleidsmakers en/ of burgers gezamenlijk experimenteren en co-creëren.

4. Regel de ethiek van het living lab

Het living lab vindt plaats in de publieke ruimte, waardoor burgers, bewust of onbewust, onderdeel worden van het experiment. Daarom is het van belang dat er regels komen voor de ethiek van verantwoord experimenteren.

KANSEN GRIJPEN

5. Heb oog voor de mogelijkheden van digitalisering

Talloze digitale technologieën verruimen de technologische mogelijkheden enorm. Via het Internet of Things vergroten ze ons vermogen om te denken, op afstand waar te nemen en te handelen enorm. Om de kansen te grijpen dienen lokale bestuurders oog te hebben voor de technologische mogelijkheden.

6. Innoveer vanuit maatschappelijk transitieperspectief

De nieuwe opties van digitalisering bieden zowel mogelijkheden om de maatschappelijke uitdagingen van deze tijd aan te pakken als om lokale experimenten met gebruikers te ontwikkelen voor de dagelijkse praktijk en de korte termijn. Adresseren van grote gemeente overstijgende maatschappelijke opgaven zoals klimaatverandering en georganiseerde criminaliteit kan alleen als gemeentes hun lokale experimenten met elkaar verbinden.

RISICO'S VERZACHTEN

7. Heb oog voor de risico's van digitalisering in de gehele datawaardeketen

Datawaardenketens vormen fundamentele bouwblokken van de dataeconomie en datasamenleving. In deze ketens worden data verzameld en geanalyseerd en op basis daarvan wordt (steeds vaker real time) ingegrepen in onze leefwereld. Als gevolg daarvan raakt digitalisering niet alleen aan privacy en veiligheid, maar ook aan andere publieke waarden en fundamentele rechten, zoals recht-vaardigheid, menselijke waardigheid, autonomie en, niet te vergeten, controle en macht over technologie.

8. Bescherm publieke waarden via debat, beleid, technologie en organisatie

Een gezonde dataeconomie en inclusieve datasamenleving vragen om een transparante en eerlijke omgang met data. Bescherming van publieke waarden wordt geborgd door drie klassieke processen:

1. Democratisch debat en politieke besluitvorming over tal van digitale ontwikkelingen.
2. Innovatie kan met diverse beleidsinstrumenten worden gestuurd zoals regelgeving, financieel beleid en communicatie/participatie met/van burgers.
3. Ten slotte zijn technologische en organisatorische instrumenten nodig die zorg dragen voor transparantie met betrekking tot de gebruikte data en algoritmes.

SAMEN WERKEN EN LEREN

9. Innoveer samen en trek lessen uit de ervaringen rondom ICT

Op lokaal niveau is zicht noodzakelijk op de diverse experimenten die plaatsvinden. Via het totaal van experimenten, proeftuinen of living labs werkt de gemeente aan haar toekomst en laat zien hoe zij haar toekomst ziet. Coördinatie en leren 'over de projecten heen' is van groot belang. Dit geldt ook voor standaardisering en de noodzaak van kennis van ICT bij de overheid. Bij infrastructurele zaken, zoals de ontwikkeling van 'slim' licht, dient de nationale overheid het voortouw te nemen.

10. Betrek burgers bij digitalisering en wees helder over wat burgerparticipatie vermag

Aangezien digitalisering belangrijk is in het vormgeven van de toekomst, dienen burgers bij deze ontwikkeling betrokken te worden. Dit kan op traditionele wijze, maar ook via digitale middelen. Bestuurders hebben de verantwoordelijkheid om meningen en wensen uit de samenleving serieus te nemen en te laten zien op welke wijze ze daarmee omgaan. De lokale overheid moet helder zijn over verwachtingen, bevoegdheden en grenzen ten aanzien van participatie en het proces van besluitvorming.

5.7 Informatiebeveiliging

De gemeente Barneveld is al geruime tijd bezig met onderwerp Informatiebeveiliging. Op dit moment is de gemeente Barneveld bezig met de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is een zelfreguleringsinstrument en bestaat uit een set van beveiligingsmaatregelen, inclusief maatregelen die o.a. zien op de fysieke beveiliging.

De gemeente Barneveld heeft in 2017 het Informatiebeveiligingsbeleid vastgesteld. Dit beleid wordt iedere drie jaar geëvalueerd en zo nodig herzien. In het geval (beveiliging)situaties daartoe aanleiding geven, kan het Informatiebeveiligingsbeleid ook eerder aangepast worden.

Naast het Informatiebeveiligingsbeleid, stelt de gemeente Barneveld elk jaar een Informatiebeveiligingsplan op. Het Informatiebeveiligingsplan vormt een uitwerking van het Informatiebeveiligingsbeleid, waarmee per jaar de te nemen maatregelen worden vastgesteld. Verder worden in het Informatiebeveiligingsplan acties beschreven om de reeds geïmplementeerde maatregelen te waarborgen en te controleren op volledigheid en/of toepasbaarheid (Plan-, Do-, Check-, Act-cyclus). Daarnaast geldt het verantwoordingsnormenkader Eenduidige Normatiek Single Information Audit (ENSIA).

5.8 Rechten van betrokkenen

De AVG bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten zijn opgenomen in de artikelen 12 t/m 22 van de AVG. Betrokkenen, bijvoorbeeld medewerkers en inwoners, hebben het recht om na te gaan wat er met hun persoonsgegevens gebeurt en hier invloed op uit te oefenen. Wij respecteren de rechten van betrokkenen, waarmee zij hun persoonsgegevens kunnen beschermen. Om betrokkenen in staat te stellen om hun rechten te kunnen uitoefenen, worden zij hierover geïnformeerd op onze website.

Wanneer een betrokkene gebruik wenst te maken van zijn rechten onder de AVG kan de betrokkene een verzoek indienen. Dit verzoek kan schriftelijk, per e-mail of via de website van de gemeente worden ingediend. De verzoeker om informatie moet zich altijd identificeren. De informatie waarom wordt verzocht wordt kosteloos verstrekt, tenzij het verzoek buitensporig is.

Na ontvangst van een verzoek ontvangt betrokkene binnen vier weken een besluit en de informatie waarom is verzocht. Deze termijn kan met acht weken worden verlengd. Een verzoek kan worden geweigerd als het verzoek ofwel kennelijk ongegrond is ofwel buitensporig is. Tegen het besluit kan betrokkene bezwaar maken of een klacht indienen bij de Autoriteit Persoonsgegevens.

5.9 Privacy statement

Op onze website wordt in begrijpelijk en duidelijk Nederlands uitgelegd waarom wij persoonsgegevens verzamelen en verwerken, welke rechten een betrokkene heeft en waar betrokkene terecht kan met vragen en klachten.

6. Foto- en beeldmateriaal

6.1 Cameratoezicht

In de gemeente Barneveld is er cameratoezicht bij zowel gemeentelijke locaties als in de openbare ruimte. In deze paragraaf wordt aangegeven op welke locaties (mobiel) cameratoezicht plaatsvindt, met welk doel en wie voor het cameratoezicht als verantwoordelijke kan worden aangemerkt.

6.1.1 Cameratoezicht gemeentehuis, -werf en milieustraat

Wij gebruiken camera’s om de veiligheid van onze medewerkers en bezoekers te waarborgen op onze eigen locaties zoals het gemeentehuis, -werf en de milieustraat. Het cameratoezicht wordt duidelijk kenbaar gemaakt door middel van stickers en borden. Het gaat concreet om camera’s die:

- Gebouwen en eigendommen bewaken;
- Medewerkers en bezoekers beschermen;
- Helpen bij de preventie en opsporing van misdrijven waaronder diefstal en vandalisme.

6.1.2 Cameratoezicht stations

Op de stations vindt cameratoezicht plaats bij de fietsenstallingen en bij de toiletten. Bij de toiletten is cameratoezicht bij de toegang van de toiletten, op de toiletten zelf hangen geen camera's. Alleen de ingang van de toiletten wordt gefilmd. Bij zowel de fietsenstallingen als de toiletten hangen borden dat er cameratoezicht plaatsvindt. Opnames worden continu gemaakt.

Bij een incident/strafbaar feit dat gedeeld wordt met de politie wordt betrokkene hiervan niet op de hoogte gesteld, omdat achteraf het incident wordt beoordeeld en of de beelden met de politie of OM worden gedeeld (al dan niet gedwongen kader).

6.1.3 Cameratoezicht winkelgebieden en bedrijfsterreinen

Het cameratoezicht in winkelgebieden en bedrijfsterreinen valt onder de verantwoordelijkheid van Keurmerk Veilig Ondernemen Barneveld/Voorthuizen en Stichting Veiligheid en Beheer Bedrijventerreinen Barneveld (Stichting VBBB). KVO en Stichting VBBB zetten cameratoezicht in met als doel om personen, gebouwen, terreinen, zaken en productieprocessen in winkelgebieden en de

bedrijventerreinen te beveiligen. Hiervoor moeten KVO en Stichting VBBB als verantwoordelijke aantonen te voldoen aan alle wet- en regelgeving, met name op het gebied van de beveiliging van persoonsgegevens.

6.2 Pilot bodycamera's BOA

Het doel van het gebruik van de bodycamera's is om de veiligheid van de BOA's te bevorderen door de preventieve werking van de camera's. Een ander doel is het terugdringen van excessief alcoholmisbruik door jongeren en de gevolgen daarvan. De bodycamera die een BOA bij zich draagt, wordt pas ingeschakeld bij een incident als andere middelen niet toereikend zijn. Het wordt aan betrokkene medegedeeld dat er gefilmd wordt.

6.3 Gebruik van foto- en beeldmateriaal door de gemeente Barneveld

6.3.1 Foto- en beeldmateriaal van inwoners en medewerkers

Bij zowel interne als externe bijeenkomsten worden door ons zelf of door derden die wij hebben ingehuurd foto's genomen. Dat er foto's van een bijeenkomst worden gemaakt en gepubliceerd mag, mits met het volgende rekening wordt gehouden:

- Vooraf aankondigen dat er foto's worden gemaakt;
- Aangeven waarvoor de foto's worden gebruikt;
- Betrokkenen moeten de mogelijkheid hebben om niet gefotografeerd te worden als zij dit niet willen. Dit moeten betrokkenen bij de organisatie van de bijeenkomst kunnen aangeven;
- Voordat de foto's worden geplaatst worden deze gereviewed. Wanneer dit mogelijk is worden alleen foto's gepubliceerd waarop betrokkenen niet herkenbaar op staan;
- Betrokkenen moeten de mogelijkheid hebben om achteraf foto's te laten verwijderen;
- Er wordt een bewaartermijn voor de foto's vastgelegd.

6.3.2 Stockfotografie

Bij gevoelige onderwerpen kiezen we voor stockfotografie. We zullen foto's van inwoners en/ of medewerkers nooit bij een onderwerp plaatsen dat een negatieve associatie heeft of kan hebben. We kopen dan een rechten vrij beeld aan, specifiek voor het onderwerp. Denk hierbij bijvoorbeeld aan een foto op de gemeentelijke website voor schuldhulpverlening of een foto voor een folder over ziekteverzuim.

6.4 Social Media

Door het team Communicatie is een Social Media beleid opgesteld en deze staat op intranet.

7. Incidenten met betrekking tot persoonsgegevens

7.1 Melding en afhandeling

Sinds 1 januari 2016 geldt de meldplicht datalekken[19]. Deze meldplicht houdt in dat organisaties direct een melding moeten doen bij de AP zodra zij een datalek hebben ontdekt, tenzij het niet waarschijnlijk is dat het datalek een risico vormt voor de betrokkene. Soms moet dit lek ook worden gemeld aan de betrokkene van wie de gegevens zijn gelekt.

[19] Artikel 33 en 34 AVG

Om in het geval van een datalek snel en daadkrachtig te kunnen handelen is een procedure ingericht die inwerking treedt bij aanmelding van een datalek. De beoordeling van een gemeld datalek vindt plaats door de PO, CISO en indien nodig de FG. Zij beoordelen de ernst en consequenties van een datalek en behandelen een lek vertrouwelijk. Afhankelijk van de ernst van het datalek worden door de PO het verantwoordelijke bestuursorgaan, de burgemeester of het college in de persoon van de portefeuillehouder 'Bedrijfsvoering', de directie en het betrokken afdelingshoofd geïnformeerd en geadviseerd over het datalek alvorens het datalek wordt gemeld bij de AP. Het gehele college van burgemeester en wethouders wordt geïnformeerd en geadviseerd als dat gelet op de ernst van een datalek noodzakelijk is.

Wanneer een datalek dit toelaat, dan wordt het verantwoordelijke bestuursorgaan, de burgemeester of het college in de persoon van de portefeuillehouder 'Bedrijfsvoering, de directie en het betrokken afdelingshoofd bij kennisgeving geïnformeerd. Deze kennisgeving gebeurt geanonimiseerd, tenzij dit omwille van de afhandeling van het datalek niet mogelijk is.

Een datalek kan gemeld worden via datalek@barneveld.nl.

7.2 Registratie en evaluatie

Alle datalekken worden geregistreerd in een beveiligde omgeving van Topdesk. Alleen de FG, CISO en PO hebben toegang tot deze omgeving. Het is belangrijk om incidenten in de toekomst te voorkomen door verbetermaatregelen te nemen middels evaluatie(s). Registratie van incidenten en een periodieke rapportage daarover zijn onderdeel van een professionele manier van het verwerken van persoonsgegevens. De rapportage over incidenten met betrekking tot persoonsgegevens maakt een vast onderdeel uit van het jaarverslag van de FG.

Bijlage: Bevoegdheden FG

- Betreden van ruimten: Indien het noodzakelijk is voor de uitvoering van bovengenoemde taken is de FG bevoegd om ongevraagd alle ruimten te betreden, voor zover die ruimten vallen onder de reikwijdte van het aan de FG wettelijk opgedragen toezicht.
- Vragen van inlichtingen: De FG verkrijgt alle inlichtingen die noodzakelijk zijn voor de uitvoering van bovengenoemde taken. De verwerkingsverantwoordelijke verleent alle medewerking om deze inlichtingen binnen een redelijke termijn te verstrekken. Geen medewerking hoeft te worden verleend in het geval de verwerkingsverantwoordelijke of diens ondergeschikte uit hoofde van het ambt, beroep of wettelijk voorschrift is verplicht tot geheimhouding.
- Vragen om inzage: De FG is bevoegd om inzage te vragen van zakelijke gegevens en bescheiden. Hiervan mag de FG tevens kopieën maken. Het gaat hierbij niet alleen om fotokopieën, maar ook van kopieën van (gedeelten van) geautomatiseerde gegevensbestanden. De verwerkingsverantwoordelijke moet hieraan meewerken, tenzij de verwerkingsverantwoordelijke of diens ondergeschikte uit hoofde van het ambt, beroep of wettelijk voorschrift is verplicht tot geheimhouding.
- Onderzoeken van zaken: Voor de uitvoering van bovengenoemde taken kan het betreden van ruimten soms niet voldoende zijn om toezicht uit te oefenen. Indien noodzakelijk verkrijgt de FG daarom toegang tot (computer-)systemen waarin persoonsgegevens worden verwerkt. De FG zal desnoods de beschikking dienen te krijgen over de relevante inloggegevens. Tevens zal de FG op de hoogte dienen te zijn hoe, na het inloggen, de relevante bestanden kunnen worden bevraagd.